DESIGNING HEALTHCARE DATA PRESERVATION MODEL VIA GENETICALLY MODIFIED GLOWWORM SWARM OPTIMIZATION

Annie Alphonsa M M[1] *Dr. N.Mohanasundaram*[2]

ABSTRACT

In general, Cloud computing is a computing prototype that grants energetic accessible frame especially for information, application as well as file-storing. Moreover, the prescribed model is more popular for its variety of beneficial aspects in terms of minimum consumption cost, and due to this characteristic, the technique successfully contributed almost in all areas especially in medical or healthcare sector. So, an effective analysis and extraction of information are imperative since they are facing many challenging issues. Along with this, the information or data that are in communication must be preserved to maintain its privacy needs. Hence, the privacy preservation of data is a great challenge that should be resolved expeditiously. This consideration has necessitated "a privacy-preserving algorithm in both processes: Data sanitization and Data restoration". In this context, it is planned to solve preservation issues by introducing a hybridized model termed as "Genetically-Modified Glowworm Swarm (GMGW) for both data sanitization and data restoration processes". Furthermore, the proposed scheme is evaluated over existing models with respect to certain measures and the supremacy of the proposed scheme is demonstrated.

Keywords: Cloud Computing; Healthcare sector; Data preservation; Key Generation; GMGW.

Nomenclature

Abbreviation	Description
GMGW	Genetically Modified Glowworm Swarm
GSO	Glowworm Swarm Optimization
IT	Information Technology
FF	Firefly
GA	Genetic Algorithm
ABC	Artificial Bee Colony
PSO	Particle Swarm Optimization
PccP	"Preserving cloud computing Privacy"
PPDM	"Privacy-preserving Protocol for Dynamic Medical Text Mining"
PHDA	"Priority based health data aggregation"
3PAKE	"three-party password-based Authentication Key Exchange protocol"
PPM-DDLM	"Prevent Digital Data Loss in the Cloud"
CR	Cloud Requesters

I INTRODUCTION

Cloud computing techniques often provides easier as well as simpler on-demand access from the internet [5] and are even simpler to install and sustain requiring minimum effort. Generally, Cloud computing, as the computing substructure, enables huge accessing in services, applications. Since it spreads as a vital technology milestone, a number of researchers and scientists find that the technique has ultimately altered the computing process, especially in IT fields [1][10]. Moreover, the cloud computing accessing helps the users with an inclusive resource set in various platforms, storage, etc. through internet.

Nevertheless, many cloud customers are still struggling to enjoy the benefits of cloud computing, since there are various security and privacy issues [11] [12] [13]. Further, the privacy [25] protection of data is specified as a sensational challenge in this area, and more companies and medical or healthcare [2] [20] [24] centres have processed their services related to health details [14]. The data sets portrayed in the cloud appliances are even sensitive [7] [3] [15] and accessing of health-based [19] data[4] is one of the vital needs for any researcher to analyse the study of different diseases, which must also ensure on-demand services at minimum cost [3].

The cloud faces many privacy issues which are an irritating aspect for governments and individuals [3]. Thus, the secure, as well as privacy-preserving [6] designing [16] [17] [21] [22] [23] helps in health data mining and extraction of medical images, which remains a challenging issue that

[1]Research Scholar, Department of Computer Science And Engineering Karpagam Academy of Higher Education, Coimbatore, India.

[2]HOD & Professor, Department of Computer Science And Engineering Karpagam Academy of Higher Education, Coimbatore, India.

should be effectively dealt with for an efficient solutions [1]. Certain models like "PccP model and ORUTA" [9], are there to attain cloud's privacy. However, attainment of the desired results continues to be a challenge.

This work aims to present an effective privacy-preservation approach that is highly effective in data sanitization and restoration. The paper is arranged as follows: Reviews are presented in Section II, privacy conservation model in Section III, key extraction method in Section IV, results in Section V and conclusion in Section VI.

II LITERATURE REVIEW

A. Related Works

In 2015, Jun et al. [1] developed a secure and effective privacy-preserving model termed PPDM. At first, data aggregation was proposed for the attainment of better preservation. Then, an outsourced disease modeling was also achieved. Finally, the effectiveness of the adopted scheme was proved in terms of both overhead and computational time. Liu et al., 2016 [2] developed a "privacy-preservation model with patient-centric clinical decision support system" that aided in diagnosing disease in privacy. Further, a new "additive homomorphic proxy aggregation approach" was developed for protecting the patients' detail. The efficacy of the implemented model was illustrated with a high accuracy rate. In 2015, Wei et al. [3] established a privacy-preservation model to transmit sensitive data, in which two protocols were designed that had privacy protection. The investigation took place in a realistic environment, and the model's superiority was proven.

Kuan et al. [4] in 2014 developed a PHDA approach, and the study illustrated that the developed model had attained identity, and finally, the procedure demonstrated that the PHDA had an effective delivery ratio with minimum communication costs. Further, in 2016, Sahi et al. [5] proposed two models along with the "disaster retrieval plan". Moreover, 3PAKE was adopted which finally proved that it could be used even at times of disaster. Waqar et al. [6] in 2012, reviewed the feasibility of exploiting metadata that were saved in cloud and based on database schema. At the same time, dynamic reconstruction (metadata) was also performed effectively, and the suitability of the developed approach was computed with relevant steps.

Zhang et al. [7] in 2013 developed "quasi-identifier index-based approach" that ensured conservation of data. The efficiency of the privacy-preservation approach was better than the existing approaches. Further, in 2017, Chandramohan et al. [8] reviewed the corresponding issues of intellectual and confidential information. Also, PPM-DDLM model was developed to help the CR for acquiring data stored in cloud.

III MEDICAL DATA-PRESERVATION MODEL

B. Proposed Architecture

Fig 1 illustrates the block diagram of the developed model. The objective of this model is securing sensitive medical data and it is processed in 2 phases: "(i) Data Hiding (ii) Data restoration". An optimal key is generated to perform these operations. The data that is preserved is known as sanitized data which is sent to the receiver. The receiver can access the original data only if inverse of similar key is known, and the receiver gets the hidden original data that is termed as restoration process. The retrieved original data is then exploited for clinical purposes, and especially the data from the report is sent to corresponding patients in case of critical situations.

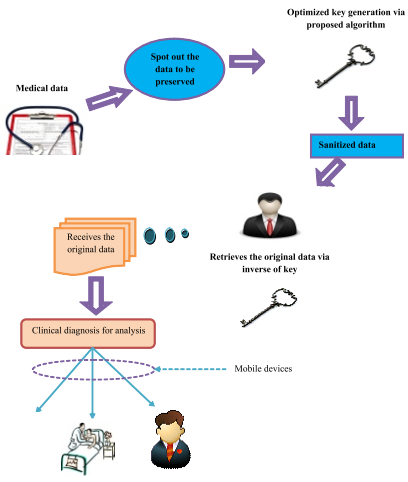

Fig. 1 Pictorial representation of the developed model

C. Data-Hiding Process

The data-hiding procedure is given in Fig 2. The generation of optimal key is given in the next section. For hiding the data, initially the optimum key is transformed into binary values. Then the clinical data is factorized with the generated value (binary) that is known as "sanitized data". The process of binary data creation is as follows: Assume data size as $_{21}SISI\times$(for example, 200 ×4), where $_{1}SI$is the records and $_{2}SI$ the fields. Let the optimum key size br 20×1 that should be factorized with the original data. Accordingly, the the converted key values should have identical length of original data. Sequentially, the element in (120) is divided into 5 sets that include 4 elements that are transformed to forty binary bits so that every subset achieves 40×4 data. "This (404) data is concatenated to get the cumulative binary data that is in the size of 200 4". This data is factorized with the original data to attain the sanitized data.

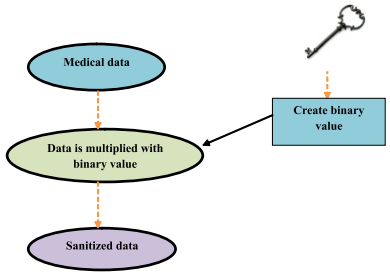

Fig. 2 Representation of data Hiding model

D. Data-Restoration procedure

The restoration procedure of proposed model is given in Fig 3. The inversion of produced optimal key includes "index as well as sensitive data". At first, a vector with the length of sanitized data is produced for sensitive data, and it is factorized with key index. Then the factorized value is summed up to sanitized data, which gives the restored data.

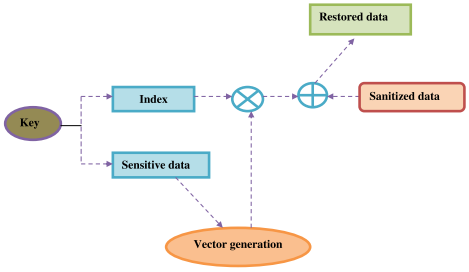

Fig. 3 Representation of data restoration process

IV Extraction of Optimal Key

E. Objective Model

The objective is to achieve the optimal key. Here, a hybridization algorithm is used namely GMGW. The key is the input solution, and chromosome length is $\frac{SI_1}{40}$ SI_2, where the limits lie between 1 to $2^{nu}-1$, in which nu denotes the bit count.

Eq. (1) describes the objective, in which DA_i symbolize original data, DA_{pi} denotes data that to be preserved, DA_{ti} denotes sanitized data, NU specifies data count.

$$\hat{F} = \min\left(OB_i\right) \tag{1}$$

$$OB_i = \frac{\sum_{i=1}^{NU} DA_{ti}}{\sum_{i=1}^{NU} DA_i} - \frac{\sum_{i=1}^{NU} DA_i - \sum_{i=1}^{NU} DA_{pi}}{\sum_{i=1}^{NU} DA_i} \tag{2}$$

F. Conventional GSO Model

GSO algorithm [31] comprises four phases "(i) Initialization (ii) Luciferin-update (iii) Movement (iv)Neighbourhood range Updating".

Initialization: Initially, glowworms are dispersed arbitrarily with decision domain L_0 .

Luciferin-update: If luciferin intensity is more, better position is achieved. The position of glowworm g at time ti is given by $X_g(ti)$ and respective objective function is $O\left(X_g(ti)\right)$. Afterwards apply $O\left(X_g(ti)\right)$ to $LE_g(ti)$, the level of luciferin associated to g at ti, which is given in Eq. (3), where, $LE_i(0)$ represent the luciferin decay parameter $(0 \quad 1)$ $\|$ $\|$ specifies the enhancement constant of luciferin.

$$LE_g(ti) = (1- \quad)LE_g(ti-1) + \quad \left(O\left(X_g(ti)\right)\right) \tag{3}$$

Movement: The neighbor of g glowworm must meet two facts: "(i) glowworm within decision domain of g glowworm (ii) The value of luciferin is higher over luciferin value of g glowworm". In addition, g move to l neighbour, which initiates from $Z_g(ti)$ with a prospect or probability $PR_{gl}(ti)$ as given in Eq. (4).

$$PR_{gl}(ti) = \frac{LE_l(T) - LE_g(ti)}{\sum_{k \ Z_g(ti)} LE_k(ti) - LE_g(ti)} \tag{4}$$

The evaluation of position update is specified in Eq. (5), here $size$ refers the step size.

$$X_g(ti+1) = size \quad \frac{X_l(ti) - X_g(ti)}{\| X_l(ti) - X_g(ti) \|} + X_i(ti) \tag{5}$$

Neighbourhood range update: The neighborhood update is determined as in Eq. (6), here indicate the constant.

$$L_e^g(ti+1) = \min\ L_u, \max\ 0, L_e^g(ti) + \quad |Z_g(ti)| \qquad (6)$$

G. Genetic Algorithm

GA is an optimization technique motivated by natural evolution. It includes six important steps: "(1) Crossover, (2) Mutation (3) Genotype-Phenotype Mapping (4) Selection (5) Termination".

Crossover: Definitely, the majority of species include 2 parents. The operator implements the application that relates the genetic fact of parents. Here, the crossover *po* divides into 2 solutions and accumulate them to one.

Mutation: It functions based on arbitrary variations. "The strength of disturbance or disruption is specified as mutation rate. Three foremost needs are there in mutation operator (i) reachability (ii) un-biasedness (iii) scalability".

Genotype-Phenotype Mapping: After the crossover and mutation functions, a novel offspring populace is assessed. The chromosome mappings depend on phenotype. This "genotype-phenotype mapping" avoids the bias.

Fitness: Here, the qualities of solutions are measured. The betterment of GA in solving the issues are evaluated in terms of fitness function.

Selection: "It is a process that selects the parents of a new generation, which is named as survival selection". Moreover, the mating attitude is a dynamic part, which decides "which parents must join or connect in the crossover evaluation".

Termination: It is defined when the main loop gets terminated.

H. Proposed hybrid Algorithm

This paper aims to integrate the benefits of both GA to GSO algorithms to achieve an "optimal key", by which it satisfies the objective function as defined in Eq. (2). The pseudo code of the developed GMGW is defined in Algorithm 3.

Algorithm 3: GMGW based key extraction process

Initialization
Assume $X_g(ti)$ be the position of g at ti time
Arbitrarily organize the agents
for g =1 to nu do $LE_g(0) = LE_0$
{
  $L_e^g(0) = L_0$
  Set $\max^{it}$ maximum iteration
while ti =1
  Arbitrarily generate the solutions
  Formulate fitness function
  Find best solution
while $(ti \quad \max^{it})$ do
  {
    For each g glowworm, measure $LE_g(ti)$ as per Eq. (3)
    {
      $Z_g(ti) = l : e_{gl}(ti) \quad L_e^g(ti) : LE_g(ti) \quad LE_l(ti)$;
    }
    For each g $Z_g(ti)$ does
    {
      Evaluate $PR_{gl}(ti)$ as per Eq. (4)
      l =choose glowworm ($\overline{PR}$)
      $X_g(ti+1)$ is updated as per Eq. (5)
      Evaluate fitness
      Identify best solution
      Find the distance between $X_g(ti+1)$ with global best solution
      Choose eight solutions of maximum distance
      Do crossover operation of GA for two residual solutions
      Continue the process by finding maximum distance with global best solution
      Evaluate $L_e^g(ti+1)$ as defined in Eq. (6)
    } end for
  }
  $ti = ti + 1$
}end for

V RESULTS AND DISCUSSIONS

I.Simulation setup

The implementation of adopted work was done in MATLAB 2015 a, and the outcome of the investigation was clearly observed. For this, the data used here is heart disease data, and each data is of [200 4] (200 records and 4 fields). Further, the synthetic data were generated from original data. The respective data was diverse in 10%, 20%, and 30% and creates 3 test cases: "Test case 1, Test case 2 and Test case 3. At every variation, there generated random data, i.e, for 10% variation, random data were created in the range of (-10 to +10), for 20% variation, data were created in the range of (-20 to +20), for 30% variation, data were created in the range of (-30 to +30) either by adding or subtracting the value. Thus, in each test case, there would have ten synthetic data".

At last, the suggested scheme was compared over GA [27], ABC [28], PSO [29], FF [30] and GSO [31] models. Moreover, the fitness of proposed model was analysed by varying the cross rate of GA from 0.2, 0.4, 0.6 and 0.8.

J. Sanitization Analysis

The effectiveness of sanitization process for test case 1, 2 and 3 is given in Fig. 4. From Fig. 4(a), the developed model for test case 1 has achieved effective diminution of objective function than the existing models. For data 1, the developed approach is 61.25%, 32.32%, 64.43%, 66.80% and 63.35% finer than FF, GSO, PSO, GA and ABC. At data 2, the developed model is 66.76%, 45.69%, 71.00%, 71.25% and 69.37% better than FF, GSO, PSO, GA and ABC models. From Fig. 4(b), for test case 2, the developed model for data 1 is 54.76%, 23.19%, 57.10%, 59.44% and 57.06% better from FF, GSO, PSO, GA and ABC models. For data 2, the proposed model is 43.84%, 39.94%, 48.40% and 44.61% finer than PSO, FF, GA and ABC models. Similarly, the sanitization efficiency of presented approach for test case 3 is shown by Fig. 4(c). Here, for data 1, the presented scheme is 54.71%, 15.78%, 58.50%, 60.94% and 58.09% superior to FF, GSO, PSO, GA and ABC models. The overall performance of the developed model shows that in terms of sanitization process it is better than other models.

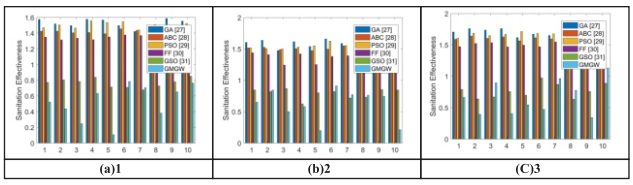

Fig. 4.Sanitization efficiency of presented approach over traditional schemes for test cases (a) 1(b) 2 and (c) 3

K. Restoration Analysis

The correlations amongst the input as well as restored data is evaluated, and is highly enhanced for the developed scheme. Fig. 5 shows the restoration effectiveness of the developed as well as existing models for all test cases. From Fig. 5(a), it is known that the developed model for data 1 is 5.13%, 2.15%, 4.83%, 5.01% and 4.01%, superior to FF, GSO, PSO, GA and ABC models. In Fig. 5(b), the adopted scheme is 4.14%, 0.38%, 5.61% and 3.52% superior to FF, GSO, GA and PSO models for 1st data. For data 2, the adopted scheme is 4.57%, 4.70%, 1.59%, 6.00% and 4.44% superior over GA, FF, GSO, PSO and ABC models. Likewise, from Fig. 5(c), the developed model for data 1 is 4.06%, 1.38%, 6.16%, 5.18% and 5.80%, superior over FF, GSO, PSO, GA and ABC models. Thus, a better restoration process is found to be achieved by the developed model over the existing models.

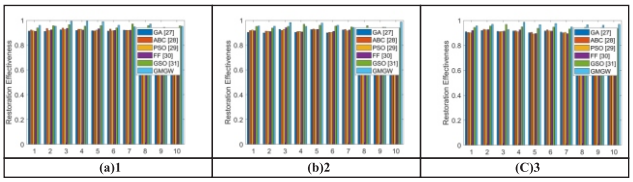

Fig. 5.Restoration efficiency of presented approach over traditional schemes for test cases (a) 1(b) 2 and (c) 3

L. Statistical analysis

In general, "metaheuristic algorithms are stochastic in nature, and hence the attaining of accurate result is quite difficult, and it is necessary to define the best, worst, mean, median and standard deviation". Fig. 6 reveals the statistical examination of adopted and traditional schemes for test case 1. From Fig. 6 (a), it is proved that the presented GMGW under best case scenario is 70.21%, 32.78%, 73.62%, 73.95% and 73.23% superior to FF, GSO, PSO, GA and ABC models. Similar examination is done for test cases 2 and 3 as revealed in Fig. 6(b) and Fig. 6(c). Finally, the analysis shows that the presented framework performs better than the existing approaches

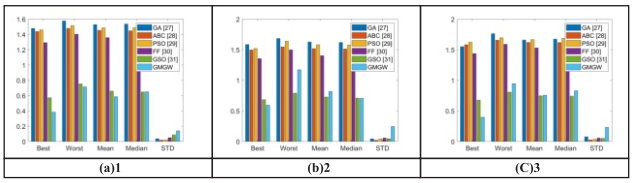

Fig. 6.Statistical investigation of presented approach over traditional schemes for test cases (a) 1(b) 2 and (c) 3

M. Convergence analysis

The convergence analysis of the presented model over traditional models is shown by Fig.7 for 3 test cases. Here,

the cost functions is found to be minimal with increase in iterations. The proposed model has attained converged cost function, especially at 100th iteration, a much minimal cost has been achieved by the adopted scheme. Similar results are observed for test cases 2 and 3. This demonstrates the superiority of the adopted scheme in minimizing the cost function over the existing methods.

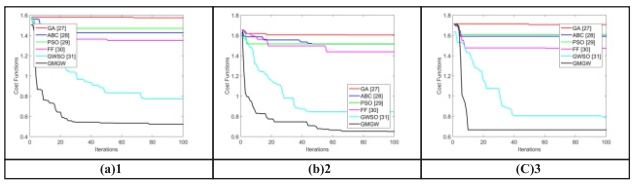

Fig. 7.Convergence analysis of presented approach over traditional schemes for test cases (a) 1(b) 2 and (c) 3

N. Analysis on Fitness

The analysis on fitness for the implemented GMGW approach is revealed in Fig. 8. Here, the analysis was carried out by varying the cross rate from 0.2, 0.4, 0.6 and 0.8. On analysing the outcomes from Fig. 8, the value of fitness attained when is found to be minimal compared to the values attained when =0.2, 0.4 and 0.6 for 2nd test case. While noticing the analysis outcome for 3rd test case, the value of fitness attained when is found to be minimal compared to the values attained when =0.2, 0.4 and 0.6. Thus, minimal fitness is achieved by the presented model.

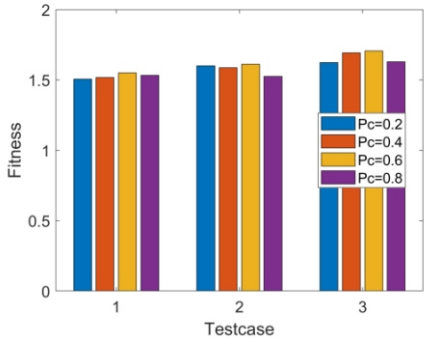

Fig. 8.Analysis on fitness of proposed model by varying the cross rate

O. Key sensitivity

By varying the level of key to 10%, 30%, 40%, 50% and 70%, the optimal key sensitivity is analyzed. The developed scheme has achieved enhanced outcomes for all variations with least correlation. From Table I, the key sensitivity of GMGW model for test case 1 is 6.89%, 3.57%, 4.70%, 2.40% GA, ABC, PSO, and FF models at 30% variation. For 40% variation, the adopted scheme is 11.25%, 8.97%, 8.97%, 10.12% and 7.79% better from ABC, GA, PSO, GSO and FF models. Concerning test case 2, the developed scheme for 30% variation is 16.17%, 1.72%, 14.92%, 19.71% and 5% superior to ABC, GA, PSO, GSO and FF models. Thus, the overall examination gives the betterments of presented scheme over existing schemes.

Table I. Key Sensitivity of Presented Approach Over Traditional Schemes by Varying % of Key for Test Cases (a) 1(b) 2 and (c) 3

Variation of key (%)	GA [27]	ABC[28]	PSO[29]	FF [30]	GSO[31]	GMGW
Test case 1						
10	0.92557	0.91811	0.92848	0.90306	0.91186	0.92557
30	0.7658	0.80516	0.79435	0.79518	0.8002	0.7658
40	0.82418	0.8335	0.87724	0.8115	0.85525	0.82418
50	0.74104	0.72784	0.72617	0.72557	0.75785	0.74104
70	0.46935	0.50639	0.52598	0.54074	0.57868	0.46935
Test case 2						
10	0.99086	0.99183	0.99315	0.98825	0.98863	0.99086
30	0.88629	0.88314	0.87222	0.85917	0.85913	0.88629
40	0.76169	0.82616	0.82631	0.77147	0.84854	0.76169
50	0.67548	0.66172	0.72057	0.68691	0.74422	0.67548
70	0.67117	0.67092	0.69726	0.68584	0.70252	0.67117
Test case 3						
10	0.99984	0.9998	0.99985	0.99982	0.99981	0.99984
30	0.77396	0.74687	0.81461	0.7779	0.78458	0.77396
40	0.70573	0.73478	0.76758	0.73486	0.74327	0.70573
50	0.76752	0.79752	0.80036	0.77944	0.80824	0.76752
70	0.74719	0.80194	0.80049	0.7336	0.79099	0.74719

VI CONCLUSION

An effective privacy preservation model was developed in this paper, by which sensitive healthcare data could be highly preserved. To do the sanitization process, a hybridized model named as GMGW was proposed. Further, the proposed GMGW was evaluated comparing it with the existing models proving its superiority regarding certain analyses like statistical analysis, convergence analysis and so on. Particularly, the key sensitivity of GMGW model for test case 1 was 6.89%, 3.57%, 4.70%, 2.40% GA, ABC, PSO, and FF models at 30% variation. For 40% variation, the adopted scheme was 11.25%, 8.97%, 8.97%, 10.12% and 7.79% better from ABC, GA, PSO, GSO and FF models. Concerning test case 2, the developed model for 30% variation was 16.17%, 1.72%, 14.92%, 19.71% and 5% superior to ABC, GA, PSO, GSO and FF models. Thus, the superiority of the adopted scheme was proved from the simulation outcomes.

References

[1] J. Zhou, Z. Cao, X. Dong and X. Lin, "PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems," IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1332-1344, Oct. 2015.

[2] X. Liu, R. Lu, J. Ma, L. Chen and B. Qin, "Privacy-Preserving Patient-Centric Clinical Decision Support System on Naïve Bayesian Classification," IEEE Journal of Biomedical and Health Informatics, vol. 20, no. 2, pp. 655-668, March 2016.

[3] WeiWang, LeiChen and QianZhang," Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation", Computer Networks, vol. 88, pp. 136-148, 2015.

[4] KuanZhang, XiaohuiLiang, . MrinmoyBaura, RongxingLu and Xuemin (Sherman)Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs", Information Sciences, vol. 284, pp. 130-141, 2014.

[5] Aqeel Sahi, David Lai and Yan Li," Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan", Computers in Biology and Medicine, vol. 78, pp. 1-8, 2016.

[6] Adeela Waqar, Asad Raz, Haider Abbas and Muhammad Khurram Khan," A framework for preservation of cloudusers' data privacy using dynamic reconstruction of metadata", Journal of Network and Computer Applications, vol. 36, pp. 235–248, 2013.

[7] XuyunZhang, ChangLiu, SuryaNepal and injunChen," An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud", Journal of Computer and System Sciences, vol. 79, no.5, pp. 542-555, 2013.

[8] ChandramohanDhasarathan, . VengattaramanThirumal, Dhavachelvan and Ponnurangam, " A secure data privacy preservation for on-demand cloud service", Journal of King Saud University - Engineering Sciences, vol. 29, no. 2, pp. 144-150, 2017.

[9] Mr. R. Nallakumar,Dr. N. Sengottaiyan, M.MohamedArif, " CLOUD COMPUTING AND METHODS FOR PRIVACY PRESERVATION: A SURVEY", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 3, no. 11, 2014.

[10] L. Gatzoulis and I. Iakovidis, "Wearable and Portable eHealth Systems," IEEE Engineering in Medicine and Biology Magazine, vol. 26, no. 5, pp. 51-56, Sept.-Oct. 2007

[11] H. Takabi, J. B. D. Joshi and G. J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no.6, pp. 24-31, Nov.-Dec. 2010.

[12] DimitriosZissis and . Author links open the author workspace. Dimitrios Lekkas," Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no.3, pp. 583-592, 2012.

[13] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, March-April 2011.

[14] S. H. Lee, J. H. Song and I. K. Kim, "CDA Generation and Integration for Health Information Exchange Based on Cloud Computing System," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 241-249, March-April 1 2016.

[15] IliasIakovidis," Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe", International Journal of Medical Informatics, vol. 52, no. 1-3, pp. 105-115, 1998.

[16] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621-1631, Sept. 2012.

[17] Haoran Li, Li Xiong, Lucila Ohno-Machado and Xiaoqian Jiang, " Privacy Preserving RBF Kernel Support Vector Machine", BioMed Research International, vol. 2014, pp. 1-10, 2014.

[18] H. Monkaresi, R. A. Calvo and H. Yan, "A Machine Learning Approach to Improve Contactless Heart Rate Monitoring Using a Webcam," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1153-1160, July 2014.

[19] A.Azadeh,I.M.Fam, M.Khoshnoud and M.Nikafrouz," Design and implementation of a fuzzy expert system for performance assessment of an integrated health, safety, environment (HSE) and ergonomics system: The case of a gas refinery", Information Sciences, vol. 178, no. 22, pp. 4280-4300, 2008.

[20] M. Barua, X. Liang, R. Lu, X. Shen, "ESPAC:Enabling security and patient-centric access control for ehealth in cloud computing", International Journal of Security and Networks, vol. 6 , no.2-3, pp. 67–76, 2011.

[21] R. Lu, X. Lin and X. Shen, "SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks," 2010 Proceedings IEEE INFOCOM, pp. 1-9, 2010.

[22] E. Shi, T. Chan, E. Rieffel, R. Chow, D. Song, "Privacy-preserving aggregation of time-series data", Proc. NDSS, 2011.

[23] J. Shi, R. Zhang, Y. Liu and Y. Zhang, "PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems," 2010 Proceedings IEEE INFOCOM, San Diego, CA, pp. 1-9, 2010.

[24] H. Viswanathan, B. Chen and D. Pompili, "Research challenges in computation, communication, and context awareness for ubiquitous healthcare," IEEE Communications Magazine, vol. 50, no. 5, pp. 92-99, May 2012.

[25] K. Zhang, X. Liang, X. Shen and R. Lu, "Exploiting multimedia services in mobile social networks from security and privacy perspectives," IEEE Communications Magazine, vol. 52, no. 3, pp. 58-65, March 2014.

[26] Yongquan Zhou, Guo Zhou, Yingju Wang and Guangwei Zhao, "A Glowworm Swarm Optimization Algorithm BasedTribes", Applied Mathematics and Information ciences, vol.7, no. 2L, pp.537-541, 2013.

[27] JohnMcCall, " Genetic algorithms for modelling and optimisation", Journal of Computational and Applied Mathematics, vol. 184, no. 1, pp. 205-222, 2005.

[28] D.KarabogaB.Basturk, " On the performance of artificial bee colony (ABC) algorithm", Applied Soft Computing, vol. 8, no. 1, pp. 687-697, 2008.

[29] M.R.Tanweer, S.Suresh, and N.Sundararajan, " Self regulating particle swarm optimization algorithm", Information Sciences, vol. 294, pp. 182-202, 2015.

[30] IztokFister, IztokFisterJr, Xin-SheYang and JanezBrest, " A comprehensive review of firefly algorithms", Swarm and Evolutionary Computation, vol. 13, pp. 34-46, 2013.

[31] BinWu, CunhuaQian, WeihongNi and ShuhaiFan, " The improvement of glowworm swarm optimization for continuous optimization problems", Expert Systems with Applications, vol. 39, no. 7, pp. 6335-6342, 2012.